(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 965 988 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
19.10.2005 Bulletin 2005/42

(51) Int Cl.^{7}: **G11B 20/00**, G11B 20/12, G11B 23/28

(21) Application number: **99304620.0**

(22) Date of filing: **14.06.1999**

(54) Write protection method for an optical disc

Schreibschutzverfahren für eine optische Platte

Procédé de protection d'écriture pour un disque optique

(84) Designated Contracting States:
DE FR GB NL

(30) Priority:

15.06.1998	**KR 9822390**
24.06.1998	**KR 9823917**
24.09.1998	**KR 9839727**
10.12.1998	**KR 9854190**
10.02.1999	**KR 9904679**

(43) Date of publication of application:
22.12.1999 Bulletin 1999/51

(60) Divisional application:
03002191.9 / 1 315 163
03002192.7 / 1 308 950
03002193.5 / 1 308 951
03002194.3 / 1 306 840
03002195.0 / 1 306 841

(73) Proprietor: **SAMSUNG ELECTRONICS CO., LTD.**
Suwon-City, Kyungki-do (KR)

(72) Inventors:
- **Ko, Jung-wan**
  Yongin-city, Kyungki-do (KR)
- **Lee, Kyung-geun**
  Bundang-gu, Sungnam-city, Kyungki-do (KR)

(74) Representative: **Chugg, David John et al**
Appleyard Lees,
15 Clare Road
Halifax, West Yorkshire HX1 2HY (GB)

(56) References cited:

EP-A- 0 406 021	**EP-A- 0 921 526**
WO-A-96/28820	**US-A- 4 805 061**
US-A- 5 617 393	**US-A- 5 654 950**

- **ANONYMOUS: "Method for Write-Protecting a Program Disk" IBM TECHNICAL DISCLOSURE BULLETIN, vol. 30, no. 10, March 1988 (1988-03), page 62 XP000073358 New York, US**
- **PATENT ABSTRACTS OF JAPAN vol. 1997, no. 03, 31 March 1997 (1997-03-31) & JP 08 315361 A (RICOH CO LTD), 29 November 1996 (1996-11-29)**
- **PATENT ABSTRACTS OF JAPAN vol. 1999, no. 05, 31 May 1999 (1999-05-31) & JP 11 045545 A (SONY CORP), 16 February 1999 (1999-02-16)**
- **PATENT ABSTRACTS OF JAPAN vol. 1998, no. 01, 30 January 1998 (1998-01-30) & JP 09 231018 A (SONY CORP), 5 September 1997 (1997-09-05)**

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to write protection methods for optical discs and particularly, though not exclusively, for protecting data recorded by a user on a write-once or rewritable medium from unwanted overwriting or erasing.

[0002] A DVD-R (Digital Versatile Disc-Recordable) standard and a WORM (Write Once Read Many) standard are standards for a write-once disc, and a DVD-RAM (Digital Versatile Disc Random Access Memory) standard and a DVD-RW (Digital Versatile Disc-Rewritable) standard are standards for a rewritable disc.

[0003] According to the DVD-RAM standards published in July of 1997, *DVD Specifications for Rewritable Disc, Part 1 Physical Specifications Version 1.0,* a DVD-RAM adopts a cartridge containing a disc, and discs from Type 2 and Type 3 cartridges can be used, after removal from the cartridge, as bare discs.

[0004] Three types of cartridges for a DVD-RAM are defined as follows. In the Type 1 cartridge, a single sided disc or double sided disc is installed in the cartridge and the installed disc can not be taken out of the case. In the Type 2 cartridge, a single sided disc is installed and the installed disc can be taken out of the case. However, when the disc is taken out of the case once, a sensor hole capable of sensing the removal of the disc is permanently changed into an open state, so that the sensor hole cannot be changed into a closed state again. Thus, it can be determined whether or not the disc has been taken out of the case. Also, in the Type 3 cartridge, a sensor hole capable of determining whether or not a disc has been taken out of the case is open at the early stage, so the disc can be taken out of or put into the case without restrictions.

[0005] Also, the cartridge has a write-inhibit hole (alternatively called "recognition switch for write protection") and according to the standard at page PH-69 page writing is possible when the write-inhibit hole is closed and is impossible when the write-inhibit hole is open. That is, when a user intends to protect data written by the user from unwanted overwriting or erasing, the corresponding write-inhibit hole in a closed state is changed into an open state, such that a recording apparatus cannot record to the disc of the corresponding cartridge.

[0006] However, in the case of using the Type 2 or Type 3 cartridge, a bare disc can be used without the case as described above. This is so the disc can be used in a thin recording/reproducing apparatus such as a laptop computer which cannot adopt a cartridge. However, the above specifications do not define any write-protect means other than the write-inhibit hole attached to the case of the cartridge.

[0007] For example, when a user, after removing a disc installed in a case that protects from writing, inserts the disc into to a thin recording/reproducing apparatus that cannot accept a cartridge, the write protection by the write-inhibit hole is no longer effective.

[0008] Also, there are many DVD related specifications such as DVD-ROM specification (DVD specification for Read Only Memory), DVD-R specification (DVD specification for Recordable Disc) . Also, many specifications for rewritable DVD, which are not established yet, can be considered, e.g., DVD specification for rewritable and readable disc, which is very similar to the DVD-R specification, and DVD specification for disc with enhanced density. Such a series of specifications with the prefix of DVD are called "DVD family".

[0009] Also, a computer operating system adopts various attributes, e.g., read-only and write protection, which is capable of preventing an arbitrary change in written data using attributes of a file that stores the data. However, when a disc is managed at a level lower than that of a file system for managing file, for example, when the recording and reproduction are directly performed, not via the file system, when the disc is initialized, where the entire file system may not be referred, or in the case that attributes of each file cannot be considered, such a method is not a perfect protection method. A method of protecting data of a bare DVD-RAM from unwanted overwriting or erasing has not yet been introduced.

[0010] In the case of a DVD-RAM, a disc can be used in a bare state as well as with the case on. However, in the case of DVD-R or DVD-RW, a disc in a case cannot be used, so that the need to protect the bare disc from unwanted overwriting or erasing has increased. However, when a bare disc taken out of a case is used, it is not possible to utilize the write-inhibit hole, so the write protection must be provided on the disc itself.

[0011] In the DVD-R specification, a 3.95GB specification (Version 1.0) and a 4.7GB specification (final draft, Version 1.9) do not mention a write protection method for a bare disc. Meanwhile, DVD-RW specifications are being prepared based on the DVD-R specification, and particularly, Version 1.9 defines the use of a bare disc without a case. However, if a future specification defines the use of a disc in a case (for example, extension of application), there will be no write protection method to be applied to a bare disc since the conventional write protection method, which has been applied to a DVD-RAM using the write-inhibit hole, is used.

[0012] If the DVD-RW specification allows the use of a case, writing can be prevented using a write-inhibit hole as in the DVD-RAM. However, if a user forgets to change the write-inhibit hole into a write-inhibit position, unwanted erasing or overwriting of data can occur.

[0013] EP-A-0 406 021 discloses a recordable and/or rewritable optical recording medium, the medium including a Lead-in area, a Lead-out area and a user data area wherein the recording medium stores a write protection information capable of protecting the data recorded on the recording medium from unwanted overwriting or erasing.

[0014] It is an aim of embodiments of the present invention to provide a write protection method for a recording and/or reproducing apparatus, capable of protecting information written on a recordable and/or rewritable medium from being undesirably overwritten or erased.

[0015] According to the present invention, there is provided a write protection method for an optical disk for an optical disc recording and/or reproducing apparatus, wherein data recorded on a recordable and/or reproducible recording medium including a Lead-in area, a Lead-out area and a user data area is protected from unwanted overwriting or erasing, the method comprising: (a) checking write-protection information stored on the recording medium; and (b) prohibiting writing of data on the recording medium according to the write-protection information; wherein the write protection information is stored in disc identification zones of at least one of the Lead-in area and the Lead-out area of the recording medium; characterised in that the method comprises the further steps of: (c) step (a) comprises reading at least two redundantly stored write protection information data from the recordable and/or reproducing recording medium; (d) comparing the read write protection information for a match; and (e) determining whether the recordable and/or reproducible recording medium is set to a write protection state based upon whether a match is detected.

[0016] Suitably, the method further comprises the steps of: (c) determining whether the write-protection information is hard write protection information; and (d) prohibiting writing of data on the entire recording medium if the write protection information is the hard write protection information, and otherwise allowing the writing of data in the user data area.

[0017] Suitably, the method further comprises the steps of: (e) determining whether the write-protection information is soft write protection information; and (f) prohibiting writing of data on the entire recording medium except for a part of the recording medium, and otherwise allowing the writing of data in the user data area.

[0018] Suitably, the method further comprises the steps of: (g) determining whether the write protection information is for a specific region of the user data area; and (h) prohibiting the writing of data in the specific area if the write protection information is for the specific area, and otherwise allowing the writing of data in the user data area.

[0019] Suitably, the method further comprises the steps of: (i) determining whether the recording medium is installed in a case; (j) if the recording medium is installed in the case, checking whether or not the case is set to a write protection state; and (k) if the write protection information of the recording medium checked in the step (a) does not match the write protection state of the case, informing a user of the difference.

[0020] Suitably, the method further comprises the step of (i) prohibiting the writing of data in the recording medium if the write protection information of the recording medium checked in the step (a) or the write protection state of the case checked in the step (j) is set to the write protection state.

[0021] Suitably, the method further comprises the steps of: (m) checking the write protection state set in the recording medium; and (n) updating the write protection information set in the recording medium to a write protection state or a write protection release state according to the write protection information set by a user.

[0022] Suitably, the step (n) comprises the sub-steps of: (n1) if the user sets the write protection state, updating the write protection information to the write protection state, and if the user sets the write protection release state, determining whether the recording medium is set to a hard write protection state; and (n2) if the recording medium is set to the hard write protection state, informing the user of that releasing the write protection is impossible, and otherwise updating the write protection information to the write protection release state.

[0023] Suitably, the method further comprises the step of (o) if the write protection information of the recording medium, set by the user, and the write protection state of the case do not match, informing the user of the difference.

[0024] For a better understanding of the invention, and to show how embodiments of the same may be carried into effect, reference will now be made, by way of example, to the accompanying diagrammatic drawings in which:

Figure 1 is a perspective view of a cartridge for a DVD-RAM (Digital Versatile Disc Random Access Memory), having a write-inhibit hole;

Figure 2 shows the structure of a general DVD-RAM;

Figures 3A and 3B show the data structure of a defect management area (DMA) of a general DVD-RAM;

Figures 4A and 4B show examples of the data structure of the DMA of a DVD-RAM, for storing write protection information, for use in embodiments of the present invention;

Figures 5A and 5B show further examples of the data structure of the DMA of a DVD-RAM, for storing write protection information, for use in embodiments of the present invention;

Figure 6 is a flowchart illustrating a write protection method according to a preferred embodiment of the present invention;

Figure 7 is a flowchart illustrating a method of updating write protection information according to an embodiment of the present invention;

Figure 8 shows the structure of the disc identification zone for storing the write protection information for use with the present invention;

Figure 9 shows the data structure of the write protection information stored in the disc identification zone of Figure 8;

Figure 10 shows the structure of a disc satisfying general DVD-R and DVD-RW specifications;

Figure 11 shows the structure of the Lead-in area shown in Figure 10;

Figure 12 shows the structure of the control data zone shown in Figure 11;

Figure 13 shows the contents of the RMD (Recording Management data) field of an RMA (Recording Management Area) according to the DVD-R and DVD-RW specifications;

Figure 14 shows the contents of the conventional RMD field 0 shown in Figure 13;

Figure 15 shows the contents of the RMD field 0 for storing the write protection information for use with an embodiment of the present invention; and

Figure 16 is a flowchart illustrating a write protection method according to another embodiment of the present invention.

[0025] Referring to Figure 1, where the write-inhibit hole of a cartridge according to the DVD-RAM specification is shown, reference numeral 1 represents a write-inhibit hole and a reference numeral 2 represents a sensor hole used to determine whether a disc has been taken out of a case.

[0026] In Figure 1, the closed write-inhibit hole 1 indicates that writing is allowed, and an open write-inhibit hole 1 indicates that writing is prohibited. Thus, when the write-inhibit hole 1 is opened, in the corresponding DVD-RAM recording/reproducing apparatus, writing of data to a disc is prohibited even if a write command is input from the outside, so that information written on the disc can be protected from unwanted overwriting.

[0027] Figure 2 shows the structure of a disc according to the DVD-RAM specification. The disc is comprised of three parts, i.e., a Lead-in area, a user data area and a Lead-out area, in the aspect of function. Also, the disc can be classified into a rewritable area and an unwritable area. In particular, the Lead-in area contains a read-only zone in the innermost part, which is an unwritable embossed data zone having pits, and a rewritable data zone following the read only zone, in which both recording and playback are possible. Meanwhile, the Lead-out area and the user data area comprise only the rewritable data zone. The read-only zone of the Lead-in area contains information about physical specifications of the disc. The rewritable data zone of the Lead-in area and the Lead-out area contain four defect management areas DMA 1, DMA 2, DMA 3 and DMA 4 in which information about disc defects is written, a disc test zone for use by a disc manufacturer in checking the status of the disc, a drive test zone for testing recording and reproduction operations in a recording/reproducing apparatus, a guard track zone for connecting each zone, and a disc identification zone.

[0028] In the DVD-RAM specification version 1.0, the purpose in use of the disc identification zone and the content thereof are not yet clearly described.

[0029] Figures 3A and 3B show the data structure in the defect management area (DMA) described at pages PH-155 through PH-158 of the DVD-RAM specification, particularly, and in particular, they show the data structure of a disc certification flag and a group certification flag respectively, in a disc definition structure (DDS) area.

[0030] A total of four defect management areas DMA 1, DMA 2, DMA 3 and DMA 4 are present in the Lead-in area and the Lead-out area of a disc, wherein DMA 1 and DMA 2 exist in the Lead-in area and DMA 3 and DMA 4 exist in the Lead-out area, and identical information relating to disc defects and initialization of the disc is stored in each area. Writing such identical information in different areas, i.e., in two areas DMA 1 and DMA 2 of the Lead-in area and in two areas DMA 3 and DMA 4 in the Lead-out area, is done to prevent the problem of data becoming unusable due to disc defects.

[0031] In the byte position 3, i.e., BP3, of the disc definition structure (DDS), a disc certification flag as shown in Figure 3A is present, and the disc certification flag comprises "In Process" information indicating the initialization state of the disc, a "User certification" flag indicating whether the disc is certified by a user, and a "Disc manufacturer certification" flag indicating whether the corresponding disc is certified by a disc manufacturer, and flag information written in the byte position BP3 is information about the entire disc.

[0032] Also, in the byte positions 16 to 39, BP16~BP39, each byte has a group certification flag as shown in Figure 3B in an identical configuration. The byte positions BP16~BP39 have initialization information about 24 recordable areas, i.e., a group, defined in the DVD-RAM specification version 1.0. That is, each group certification flag has "In Process" information indicating the initialization state of the corresponding group and a "User certification" flag indicating whether the disc is certified by a user. Here, the group refers to specific recordable areas of the disc.

[0033] Figures. 4A and 4B are examples of the data structures of a disc certification flag and a group certification flag of the disc definition structure (DDS) area of the defect management area (DMA) that stores write protection information according to the present invention. In the data structure of the disc certification flag shown in Figure 4A, "Disc write protection" information is stored in bits b4 and b3 of a reserved disc certification flag "Reserved", in contrast to the data structure of the disc certification flag shown in Figure 3A, and is defined as follows.

	Disc write protection
b4, b3 = 00b	Disc is not write protected
10b	Disc is write protected Entire disc shall not be written to except for drive test area, and DMA area
11b	Disc is write protected Entire disc shall not be written to These bits shall not be modified to other values
Others	Reserved

[0034] In the same manner, the data structure of the group certification flag shown in Figure 4B stores "Group write protection" information in bits b4 and b3 of a reserved group certification flag "Reserved", in contrast to the data structure of the group certification flag shown in Figure 3B, and is defined as follows.

	Group write protection
b4, b3 = 00b	Group is not write protected
10b	Group is write protected. User data shall not be written to this block
Others	Reserved

[0035] The states of the bits b4 and b3 of the disc certification flag, and those of the bit b4 and b3 of the group certification flag are shown in Table 1.

Table 1

disc certification flag		group certification flag		states
b4	b3	b4	b3	
0	0	0	0	No write protection
0	0	1	0	Given group is write protected
1	0	Don't care		Soft write protected on entire disc
1	1			Hard write protected on entire disc

[0036] In the above Table 1, soft write protection means that write protection can be released, that is, that the write protection state can be changed to a rewritable state by setting the corresponding bit b4 to "0". Also, hard write protection means that write protection is applied to the Lead-out area as well as to the Lead-in area, so that the write protection state can not be restored to the rewritable state.

[0037] In the hard write protection for the group, making a part of the disc hard write-protected does not provide advantages to a user in use, rather than in a technical aspect, and particularly there is a problem of processing in the corresponding group when the entire disc is reinitialized. Thus, it is unfavorable to set the hard write protection for the group.

[0038] As shown in the data structure of Figures. 4A and 4B, the write protection information of the disc is written in the disc definition structure (DDS) of the defect management area (DMA), and identical write protection information is written four times to the same disc, so that robustness of the write protection information on the disc is enhanced.

[0039] When a bare disc that is write protected is inserted for use into a case, the write-inhibit hole of which is in a rewritable state, or if a bare disc that is not write protected is inserted into a case, the write-inhibit hole of which is in a write protection state, the write inhibition information stored on the disc cannot match the state of the write-inhibit hole of the case.

[0040] In such a case, if either one of the disc or the case is write protected, it is preferable to operate to be suitable for the write protection state. This is because in the user's position it is preferable that the content of data is checked again without overwriting rather than the important data being damaged through overwriting.

[0041] Figures 5A and 5B are further examples of the data structures of the disc certification flag and the group certification flag, respectively, of the disc definition structure (DDS) area of the defect management area (DMA) that stores the write protection information.

[0042] In the case where the write protection information is in the disc certification flag shown in Figure 5A, only one bit b4 can be used regardless of whether the write protection information is for the hard write protection or for the soft write protection, which is defined as follows.

Disc write protection	
b4 = 0b	Disc is not write protected
1b	Disc is write protected Entire disc shall not be written to except for drive test area, and DMA area

[0043] The group test flag shown in Figure 5B can store the write protection information using only one bit b4, which is defined as follows.

Group write protection	
b4 = 0b	Group is not write protected
1b	Group is write protected User data shall not be written to this block

[0044] In this case, preferably bit b4 of the disc certification flag and the bit b4 of the group certification flag are used. However, instead of using the bit b4 of the disc certification flag or group certification flag, any "Reserved" bits can be used.

[0045] Also, the bit b4 of the group certification flag, that is, "Group write protection" flag, may not be used. This is effective in a disc in which only a specific group is not write protected, and in this case the bit b4 of the group certification flag is "Reserved" as in the conventional specifications.

[0046] Figure 6 is a flowchart illustrating a write-protection method according to a preferred embodiment of the present invention. First, it is checked whether a disc is installed in a case (step S101), and if the disc is installed in the case, the state of the write-inhibit hole of the case is checked (step S102). That is, when the write-inhibit hole is closed, it means that cartridge is not write protected. When the write-inhibit hole is open, it means that the cartridge is write protected.

[0047] If it is determined in step S101 that the disc is not installed in the case, or after the state of the write-inhibit hole is checked in step S102, a write protection flag of the disc is checked (step S103). That is, write protection flags within the disc certification flag and the group certification flag are checked.

[0048] It is determined whether the write protection information of the disc matches the state of the write-inhibit hole of the case (step S104). That is, when write protection information is written on the disc and the write-inhibit hole of the case is open, it is determined whether the write protection flag of the disc certification flag is set to a "write protection" state (step S105). Otherwise, a user is informed that the write protection information of the disc does not match the state of the write-inhibit hole of the case (step S106).

[0049] If the write protection flag of the disc certification flag is set as a write protection state in the step S105, or if one of either the disc or the case indicates the write protection state even though both the write-protection states of the disc and the case do not match in the step S106, it is checked whether the disc is set to a "hard write protection" state (step S107). If the disc is set to the "hard write protection" state, data writing to the entire disc including the Lead-in area and the Lead-out area other than the user data area is prohibited (step S108). Otherwise, data writing in the user data area other than the drive test area and the defect management area (DMA) is prohibited (step S109).

[0050] If it is determined in the step S105 that the write protection flag of the disc certification flag is not set to the "writing protection" state, it is checked whether the write protection flag of the group certification flag is set to the "write protection": state (step S110). If the write protection flag of the group certification flag is set to a "write protection" state, writing data in the corresponding group is prohibited (step S111). Otherwise, data writing is allowed in the rewritable area (step S112).

[0051] The write protection method illustrated in Figure 6 corresponds to the case of using the disc certification flag containing the hard write protection flag shown in Figure 4A, and the group certification flag shown in Figure 4B. When the disc certification flag of Figure 5A and the group certification flag of Figure 5B are used, the steps S107 and S108 illustrated with reference to Figure 6 are not performed. When the disc certification flag is set to the "write protection" state in the step S105, writing data in the user data area is prohibited in step S109.

[0052] Figure 7 is a flowchart illustrating a method of setting a rewritable disc to the write protection state or of changing the write protection state of the disc to a rewritable state. A method of updating the write protection information will now be described with reference to the flowchart of Figure 7.

[0053] In Figure 7, when a disc or a cartridge is inserted into a recording/reproducing apparatus, the write protection information is checked (step S201). Then, it is determined whether the write protection information has been input by a user (step S202) and when the write protection information is input by the user, it is determined whether information set by the user is for write protection (step S203). If the information set by the user is write protection information, the corresponding write protection flag of the disc is set to the write protection state (step S204).

[0054] When the information set by the user is not write protection information in step S203, it is determined whether the information set by the user is write protection release information (step S205). If the information set by the user is the write protection release information, it is determined whether the current disc is in a hard write protection state (step S206). If the current disc is in the hard write protection state, the user is informed of that write protection cannot be released (step S207). If it is determined in step S206 that the disc is not in the hard write protection state, the corresponding write protection flag of the disc is set to the rewritable state (step S208).

[0055] Also, when the setting of the write protection or the release of the write protection of the disc is completed, that is, the step S204, S207 or S208 is completed, and the disc is installed in a case, it is determined in step S209 that the state of the write-inhibit hole of the case matches the write protection information stored in the disc. If the state of the write-inhibit hole of the case does not match the state of the disc, the user is informed of such difference (step S210), and then the procedure is completed.

[0056] The method of updating the write-protection information, illustrated in Figure 7, can be performed when a bare disc is inserted or a disc in a case is inserted, and can be performed after the write-protection is controlled using the write protection information as illustrated with reference to Figure 6.

[0057] In the preferred embodiment of a disc for use in the present invention, the write protection information of the disc is written in the defect management area of the disc. However, the disc identification zone of Figure 2 can be used instead of the defect management area of the disc. The disc identification zone is present both in the Lead-in area and the Lead-out area, like the defect management area of the disc. Thus, writing identical information two or more times to the disc identification zones located in the Lead-in area and the Lead-out area can ensure robustness as strong as in the defect management area of the disc.

[0058] Since the disc identification zone is not presently used for a specific purpose, there is an advantage that the disc identification zone does not conflict with the information written in the defect management area of the disc. In particular, information of the defect information area relates to only the DVD-RAM, it is difficult to maintain consistency between discs for optical recording/reproduction. Meanwhile, since the disc identification zone is not restricted to a specific disc, the disc identification zone can maintain consistency with another disc satisfying the similar specifications.

[0059] An example of storing the write protection information using the disc identification zone will be described with reference to Figures. 8 and 9.

[0060] As shown in Figure 8, in the structure of a disc identification zone that stores write protection information for a bare disc, four flags for write protection are concurrently written to the disc identification zone, and two or more normal flags of the four flags are read. If the contents of the read flags matches each other, it is regarded that the write protection is set for the disc.

[0061] For example, the four flags are written in only the disc identification zone of the Lead-in area, and disc identification information of 1 block length (=1 byte) is successively written four times in the four blocks from the start of the disc identification zone of the Lead-in area, and all the first bytes of disc identification information contain a write protection flag. The disc identification information of 1 block length is summarized as shown in Table 2.

Table 2

BP	Contents	Number of bytes
0	Write protection information	1 byte
1 to 32767	Reserved	32767 bytes

[0062] The write protection flag of the disc identification information corresponds to the most significant bit (MSB) of the first byte as shown in Figure 9. When the flag (indicated by "WP") value is 1b (binary), it means that the entire area of disc is write protected except for the disc identification zone and the drive test zone. Also, when the flag value is 0b, it means that the entire area of disc is rewritable. That is, "WP" of Figure 9 is defined as follows.

WP = 1b: Entire area of disc is write protected except for Drive test zone and Disc identification zone.
= 0b: Entire area of disc is not write inhibited

[0063] The reason why only two normal flags are read from the four written write protection flags is as follows. In the case where only one write protection flag is written, an error can be generated in the area in which the corresponding flag is written, so that the area cannot be used. Also, in the case where only reading and not writing is allowed, there is a possibility of abnormal operation such that no information can be written to the disc permanently by erroneously reading the corresponding flag.

[0064] Meanwhile, when writing write protection information in a plurality of locations, there is a problem in that the time required for reading the corresponding information gets longer. That is, the time required for a series of processes from the insertion of a disc, including reading various information from the disc and recognizing the information required for the control of the disc by a microcontroller, can be become longer.

[0065] However, in the case of updating the write protection information, operation only for the updating is performed. That is, because information is not read, the writing time in units of several hundreds milliseconds is barely worth consideration. Thus, writing is performed in four locations in consideration of the robustness of information, and error correction capability is taken into account during the recording. That is, if two errors are not generated, or normally corrected flags are read and two of them match each other, the write protection state of the disc is set without reading the remaining flags, thereby increasing the operating speed.

[0066] The write protection method suggested above is not limited to only the DVD-RAM, and can be applied to a disc that has specifications physically the same as DVD-R/RW and similar to the DVD specifications, which will now be described.

[0067] Figure 10 shows the structure of a disc according to general DVD-R and DVD-RW specifications. The disc is roughly divided into two parts with respect to functionality, including an R (Recording)-information area and an information area. The R-information area is divided into a PCA (Power Calibration Area) for calibrating power, and an RMA (Recording Management Area) including general information relating to recording, i.e., information about the recording mode of a disc, recording state, optimal power control and border zone, and the information area is divided into a Lead-in area, data recordable area in which data is recordable by a user and a Lead-out area that is not defined yet in the DVD-R and DVD-RW specifications.

[0068] Here, as shown in Figure 11, the Lead-in area comprises an Initial zone (contents: 00h) for which a specific purpose is not defined, a reference code zone (channel bit pattern: 3T-6T-7T) used to control an equalizer for a radio frequency signal in a drive, first and second buffer zones (contents: 00h) and a control data zone containing the contents shown in Figure 12.

[0069] In Figure 12, physical format information of the control data zone is about types and versions of the specifications, disc size, maximum transmission rate, disc structure (single/dual), recording density and data region allocation, and the disc manufacturing information is unrelated to compatibility.

[0070] Figure 13 shows the content of an RMD (Recording Management Data) field of the RMA according to the DVD-R and DVD-RW specifications. The RMA comprises a RMA Lead-in area including a system reserved field (contents: 00h) and a unique ID field, and RMD fields. As shown in Figure 13, one RMD field consists of 16 sectors, in which the first sector is allocated as a linking-loss area, general information of the disc is stored in RMD field 0, Optimum Power Control (OPC) related information is stored in RMD field 1, user specific data (contents: 00h) is stored in RMD field 2, and border zone information is stored in RMD field 3. Also, in the case of a DVD-R disc according to the specifications of version 1.9, Rzone (Recording Zone) information including recording items is stored in RMD field 4 through RMD field 12 whenever the recording is performed, and RMD field 13 and RMD field 14 are reserved.

[0071] In the case of rewritable and erasable DVD-RW disc the specifications of which are not yet defined, Rzone information is stored in RMD field 4, and RMD field 5 and RMD field 12 are allocated to store defect management & certification related information taking reliability, certification before the disc is used and management of defect in use into consideration. Also, RMD field 13 and RMD field 14 are reserved.

[0072] Figure 14 shows the contents of the general information of a disc stored in the RMD field 0 of Figure 13. In Figure 14, byte positions BP0 and BP1 stores information about RMD format (recorded only with 0001h), byte position BP2 stores information about the disc status, and byte position BP3 is reserved. The byte positions BP4 through BP21 store unique disc identifier information that stores the recording date and time of the data as ASCII code. Pre-pit information is copied over the byte positions BP22 through BP85, and the remaining byte positions BP86 through BP2047 are reserved. Here, in the DVD-R disc the disc status information stored in the byte position BP2 is defined as follows.

(BP2) Disc status
00b: Indicates that disc is empty
01b: Indicates that disc is in Disc-at-once recording mode
02b: Indicates that disc is in incremental recording mode
03b: Indicates that disc is finalized where incremental recording is used
Others: Reserved

[0073] Figure 15 is an example of a table showing the state where the write protection information is stored on the disc adopting the DVD-R and DVD-RW specifications according to the present invention using the general information of a disc stored in RMD field 0 of Figure 13.

[0074] That is, by defining the following using the reserved byte position BP3 of RMD field 0, information that the current disc is write protected can be transmitted to a drive.

(BP3) Disc write protection flag
00b: Indicates that disc is not write protected
01b: Indicates that disc is write protected (hard)
02b: Indicates that disc is write protected (soft)

[0075] Entire disc shall not be written to except for PCA, etc.

[0076] In the write protection information according to the present invention, 00b indicates that the disc is not write protected, 01b indicates that the entire disc is write protected (hard write protection), and 02b indicates that the entire disc except for a part of the disc (e.g., the PCA) is write protected (soft write protection). In the present embodiment, the write-protection information indicates that the entire disc is write protected or is not write protected. However, the RMD field of Figure 13 is written connected to the previous data whenever new data is written, so that the write-protection can be set for only the written data corresponding to the RMD.

[0077] For example, even though write protection information is stored in the byte position BP3 of RMD field 0, the write protection information on a bare disc can be written using the Lead-in area and the Lead-out area shown in Figure 10 in addition to the RMD area. Also, the byte position BP2 of RMD field 0 stores the disc status information, so that write protection information can be stored in the byte position BP2 of RMD.

[0078] Since the write protection information cannot be updated in the once-writable DVD-R, in consideration of the consistency with the DVD family, write protection information can be indicated through finalization that means the writing on the defined Lead-in area and Lead-out area. That is, that the finalization is completed indicates the DVD-R is write-protected. Otherwise, it means that there is no write protection.

[0079] Also, as in the defect management area DMA 1, DMA 2, DMA 3 and DMA 4 of the DVD-RAM, the same content is recorded multiple times to cope with errors, thereby ensuring robustness. In the DVD-R/RW, such robustness is ensured by grouping RMDs of the RMA and providing the RMDs belonging to one group with the same content.

[0080] A disc must include format information informing whether the current disc is a DVD-R or a DVD-RW, such that a DVD-R disc and a DVD-RW disc is compatible in the same drive. As shown in Figure 15, the RMD format can be defined using the byte positions BP0 and BP1 of RMD field 0 as follows.

(BP 0,1) RMD format
0001h for R
0002h for RW
0003h for R/RW compatible mode

[0081] Figure 16 is a flowchart illustrating a write protection method according to another embodiment of the present invention, in consideration of application extension to a DVD-RW contained in a case.

[0082] First, it is determined whether a disc is installed in a case (step S301). If the disc is installed in the case, the state of a write-inhibit hole of the case is checked (step 302). That is, if the write-inhibit hole is closed, it means that cartridge is not write protected, and if the write-inhibit hole is open, it means that the cartridge is write protected.

[0083] When the disc is not installed in the case in step S301, or when the state of the write-inhibit hole is checked in step S302, the write-protection flag of the disc is checked (step S303). That is, a write protection flag within RMD field 0 is checked.

[0084] Then, it is determined whether the write protection information of the disc matches the state of the write-inhibit hole of the case (step S304). That is, when the write protection information is written on the disc and the write-inhibit hole of the case is opened, it is determined that the write protection flag is in a "write protection" state (step S305) . Otherwise, the user is informed of that the write protection information of the disc does not match the state of the write-inhibit hole of the case (step S306).

[0085] If the write protection flag of the disc is set to the "write protection" state in step S305, or after the step 306, that is, if either the disc or the case is in a "write protection" state even though the write protection information of the disc does not match the state of the write-inhibit hole of the case, it is determined whether the disc is set to the "hard write protection" state (step S307). If the disc is in the "hard write protection" state, the entire disc including the user data area is write-prohibited (step S308). Otherwise, only the user data area is write protected (step S309). Also, in the step S305 if the write protection flag is not in the "write protection" state, the disc is not write-protected (step S310).

Claims

1. A write protection method for an optical disk for an optical disc recording and/or reproducing apparatus, wherein data recorded on a recordable and/or reproducible recording medium including a Lead-in area, a Lead-out area and a user data area is protected from unwanted overwriting or erasing, the method comprising:

   (a) checking write-protection information stored on the recording medium; and
   (b) prohibiting writing of data on the recording medium according to the write-protection information;
   wherein the write protection information is stored in disc identification zones of at least one of the Lead-in area and the Lead-out area of the recording medium; **characterised in that** the method comprises the further steps of:
   (c) step (a) comprises reading at least two redundantly stored write protection information data from the recordable and/or reproducing recording medium;
   (d) comparing the read write protection information for a match; and
   (e) determining whether the recordable and/or reproducible recording medium is set to a write protection state based upon whether a match is detected.

2. The write protection method of claim 1, further comprising the steps of:

   (c) determining whether the write-protection information is hard write protection information; and (d) prohibiting writing of data on the entire recording medium if the write protection information is the hard write protection information, and otherwise allowing the writing of data in the user data area.

3. The write protection method of claim 1 or 2, further comprising the steps of:

   (e) determining whether the write-protection information is soft write protection information; and

   (f) prohibiting writing of data on the entire recording medium except for a part of the recording medium, and otherwise allowing the writing of data in the user data area.

4. The write protection method of claim 1, 2 or 3, further comprising the steps of:

   (g) determining whether the write protection information is for a specific region of the user data area; and

   (h) prohibiting the writing of data in the specific area if the write protection information is for the specific area, and otherwise allowing the writing of data in the user data area.

5. The write protection method of any preceding claim, further comprising the steps of:

   (i) determining whether the recording medium is installed in a case;

   (j) if the recording medium is installed in the case, checking whether or not the case is set to a write protection state; and

   (k) if the write protection information of the recording medium checked in the step (a) does not match the write protection state of the case, informing a user of the difference.

6. The write protection method of any preceding claim, further comprising the step of (l) prohibiting the writing of data in the recording medium if the write protection information of the recording medium checked in the step (a) or the write protection state of the case checked in the step (j) is set to the write protection state.

7. The write protection method of any preceding claim, further comprising the steps of:

   (m) checking the write protection state set in the recording medium; and

   (n) updating the write protection information set in the recording medium to a write protection state or a write protection release state according to the write protection information set by a user.

8. The write protection method of claim 7, wherein the step (n) comprises the sub-steps of:

(n1) if the user sets the write protection state, updating the write protection information to the write protection state, and if the user sets the write protection release state, determining whether the recording medium is set to a hard write protection state; and

(n2) if the recording medium is set to the hard write protection state, informing the user of that releasing the write protection is impossible, and otherwise updating the write protection information to the write protection release state.

9. The write protection method of claim 7 or 8, further comprising the step of (o) if the write protection information of the recording medium, set by the user, and the write protection state of the case do not match, informing the user of the difference.

Patentansprüche

1. Schreibschutzverfahren für eine optische Platte für eine Vorrichtung zum Beschreiben und/oder Abspielen optischer Platten, wobei Daten, die auf einem beschreibbaren und/oder abspielbaren Aufzeichnungsmedium aufgezeichnet sind, das einen Einlaufspurbereich, einen Auslaufspurbereich und einen Benutzerdatenbereich enthält, vor unerwünschtem Überschreiben oder Löschen geschützt sind, und das Verfahren umfasst:

(a) Prüfen von Schreibschutzinformationen, die auf dem Aufzeichnungsmedium gespeichert sind, und

(b) Untersagen von Schreiben von Daten auf das Aufzeichnungsmedium entsprechend den Schreibschutzinformationen;
wobei die Schreibschutzinformationen in Platten-Identifizierungszonen wenigstens des Einlaufspurbereiches oder des Auslaufspurbereiches des Aufzeichnungsmediums gespeichert sind, **dadurch gekennzeichnet, dass** das Verfahren die folgenden weiteren Schritte umfasst:

(c) Schritt (a) das Lesen von wenigstens zwei redundant gesicherten Schreibschutzinformations-Daten von dem beschreibbaren und/oder abspielbaren Aufzeichnungsmedium umfasst;

(d) Vergleichen der gelesenen Schreibschutzinformationen auf eine Übereinstimmung hin; und

(e) Feststellen, ob das beschreibbare und/oder abspielbare Aufzeichnungsmedium in einen Schreibschutz-Zustand versetzt ist, in Abhängigkeit davon, ob eine Übereinstimmung erfasst wird.

2. Schreibschutzverfahren nach Anspruch 1, das des Weiteren die folgenden Schritte umfasst:

(c) Feststellen, ob die Schreibschutzinformationen harte Schreibschutzinformationen sind; und

(d) Untersagen des Schreibens von Daten auf dem gesamten Aufzeichnungsmedium, wenn die Schreibschutzinformationen die harten Schreibschutzinformationen sind, und ansonsten Zulassen des Schreibens von Informationen in dem Benutzerdatenbereich.

3. Schreibschutzverfahren nach Anspruch 1 oder 2, das des Weiteren die folgenden Schritte umfasst:

(e) Feststellen, ob die Schreibschutzinformationen weiche Schreibschutzinformationen sind; und

(f) Untersagen des Schreibens von Daten auf dem gesamten Aufzeichnungsmedium bis auf einen Teil des Aufzeichnungsmediums, und ansonsten Zulassen des Schreibens von Daten in dem Benutzerdatenbereich.

4. Schreibschutzverfahren nach Anspruch 1, 2 oder 3, das des Weiteren die folgenden Schritte umfasst:

(g) Feststellen, ob die Schreibschutzinformationen für ein bestimmtes Gebiet des Benutzerdatenbereiches gelten; und

(h) Untersagen des Schreibens von Daten in dem bestimmten Bereich, wenn die Schreibschutzinformationen für den bestimmten Bereich gelten, und ansonsten Zulassen des Schreibens von Daten in dem Benutzerdatenbereich.

5. Schreibschutzverfahren nach einem der vorangehenden Ansprüche, das des Weiteren die folgenden Schritte umfasst:

   (i) Feststellen, ob das Aufzeichnungsmedium in einem Gehäuse installiert ist;

   (j) wenn das Aufzeichnungsmedium in dem Gehäuse installiert ist, Prüfen, ob das Gehäuse auf einen Schreibschutzzustand gesetzt ist; und

   (k) wenn die in dem Schritt (a) geprüften Schreibschutzinformationen des Aufzeichnungsmediums nicht mit dem Schreibschutzzustand des Gehäuses übereinstimmen, Informieren eines Benutzers über den Unterschied.

6. Schreibschutzverfahren nach einem der vorangehenden Ansprüche, das des Weiteren den Schritt (i) des Untersagens des Schreibens von Daten auf dem Aufzeichnungsmedium umfasst, wenn die in dem Schritt (a) geprüften Schreibschutzinformationen oder der in dem Schritt (j) geprüfte Schreibschutzzustand des Gehäuses auf den Schreibschutzzustand gesetzt ist.

7. Schreibschutzverfahren nach einem der vorangehenden Ansprüche, das des Weiteren die folgenden Schritte umfasst:

   (m) Prüfen des in dem Aufzeichnungsmedium gesetzten Schreibschutzzustandes; und

   (n) Aktualisieren der in dem Aufzeichnungsmedium gesetzten Schreibschutzinformationen auf einen Schreibschutzzustand oder einen Schreibschutz-Aufhebungs-Zustand entsprechend den von einem Benutzer gesetzten Schreibschutzinformationen.

8. Schreibschutzverfahren nach Anspruch 7, wobei der Schritt (n) die folgenden Teilschritte umfasst:

   (n1) wenn der Benutzer den Schreibschutzzustand setzt, Aktualisieren der Schreibschutzinformationen auf den Schreibschutzzustand, und, wenn der Benutzer den Schreibschutz-Aufhebungs-Zustand setzt, Feststellen, ob das Aufzeichnungsmedium auf einen harten Schreibschutzzustand gesetzt ist; und

   (n2) wenn das Aufzeichnungsmedium auf den harten Schreibschutzzustand gesetzt ist, Informieren des Benutzers, dass das Aufheben des Schreibschutzes unmöglich ist, und ansonsten Aktualisieren der Schreibschutzinformationen auf den Schreibschutz-Aufhebungszustand.

9. Schreibschutzverfahren nach Anspruch 7 oder 8, das des Weiteren den Schritt (o) des Informierens des Benutzers über den Unterschied umfasst, wenn die von dem Benutzer gesetzten Schreibschutzinformationen des Aufzeichnungsmediums und der Schreibschutzzustand des Gehäuses nicht übereinstimmen.

Revendications

1. Procédé de protection en écriture pour un dispositif d'enregistrement et/ou reproduction de disque optique, dans lequel des données enregistrées sur un support d'enregistrement enregistrable et/ou reproductible incluant une zone d'entrée, une zone de sortie et une zone de données utilisateur sont protégées d'un écrasement ou d'un effacement non-voulu, le procédé comportant les étapes consistant à :

   (a) contrôler les informations de protection en écriture mémorisées sur le support d'enregistrement, et
   (b) interdire l'écriture de données sur le support d'enregistrement conformément aux informations de protection en écriture,
   dans lequel les informations de protection en écriture sont mémorisées dans des zones d'identification de disque d'au moins l'une parmi la zone d'entrée et la zone de sortie du support d'enregistrement, **caractérisé en ce que** le procédé comporte les étapes supplémentaires suivantes :

(c) l'étape (a) comporte la lecture d'au moins deux données d'informations de protection en écriture mémorisées de manière redondante à partir du support d'enregistrement enregistrable et/ou reproductible,
(d) comparer les informations de protection en écriture lues en vue d'une concordance, et
(e) déterminer si le support d'enregistrement enregistrable et/ou reproductible est défini à un état de protection en écriture selon qu'une concordance est détectée.

2. Procédé de protection en écriture selon la revendication 1, comportant en outre les étapes consistant à :

(c) déterminer si les informations de protection en écriture sont des informations de protection en écriture strictes, et (d) interdire l'écriture de données sur le support d'enregistrement entier si les informations de protection en écriture sont des informations de protection en écriture strictes et, sinon, permettre l'écriture de données dans la zone de données utilisateur.

3. Procédé de protection en écriture selon la revendication 1 ou 2, comportant en outre les étapes consistant à :

(e) déterminer si les informations de protection en écriture sont des informations de protection en écriture souples, et
(f) interdire l'écriture de données sur le support d'enregistrement entier sauf pour une partie du support d'enregistrement et, sinon, permettre l'écriture de données dans la zone de données utilisateur.

4. Procédé de protection en écriture selon la revendication 1, 2 ou 3, comportant en outre les étapes consistant à :

(g) déterminer si les informations de protection en écriture sont destinées à une région spécifique de la zone de données utilisateur, et
(h) interdire l'écriture de données dans la zone spécifique si les informations de protection en écriture sont destinées à la zone spécifique et, sinon, permettre l'écriture de données dans la zone de données utilisateur.

5. Procédé de protection en écriture selon l'une quelconque des revendications précédentes, comportant en outre les étapes consistant à :

(i) déterminer si le support d'enregistrement est installé dans un boîtier,
(j) si le support d'enregistrement est installé dans le boîtier, contrôler si oui ou non le boîtier est défini à un état de protection en écriture, et
(k) si les informations de protection en écriture du support d'enregistrement contrôlées à l'étape (a) ne concordent pas avec l'état de protection en écriture du boîtier, informer un utilisateur de la différence.

6. Procédé de protection en écriture selon l'une quelconque des revendications précédentes, comportant en outre l'étape consistant à (i) interdire l'écriture de données dans le support d'enregistrement si les informations de protection en écriture du support d'enregistrement contrôlées à l'étape (a) ou l'état de protection en écriture du boîtier contrôlé à l'étape (j) sont définis à l'état de protection en écriture.

7. Procédé de protection en écriture selon l'une quelconque des revendications précédentes, comportant en outre les étapes consistant à :

(m) contrôler l'état de protection en écriture défini dans le support d'enregistrement, et
(n) mettre à jour les informations de protection en écriture définies dans le support d'enregistrement en les amenant à un état de protection en écriture ou à un état de désactivation de la protection en écriture conformément aux informations de protection en écriture définies par un utilisateur.

8. Procédé de protection en écriture selon la revendication 7, dans lequel l'étape (n) comporte les sous-étapes suivantes consistant à :

(n1) si l'utilisateur définit l'état de protection en écriture, mettre à jour les informations de protection en écriture en les amenant à l'état de protection en écriture, et si l'utilisateur définit l'état de désactivation de protection en écriture, déterminer si le support d'enregistrement est défini à un état de protection en écriture strict, et
(n2) si le support d'enregistrement est défini à l'état de protection en écriture strict, informer l'utilisateur que cette désactivation de la protection en écriture est impossible et, sinon, mettre à jour les informations de protection en écriture en les amenant à l'état de désactivation de protection en écriture.

9. Procédé de protection en écriture selon la revendication 7 ou 8, comportant en outre l'étape consistant à (o) si les informations de protection en écriture du support d'enregistrement, définies par l'utilisateur, et l'état de protection en écriture du boîtier ne concordent pas, informer l'utilisateur de la différence.

FIG. 1

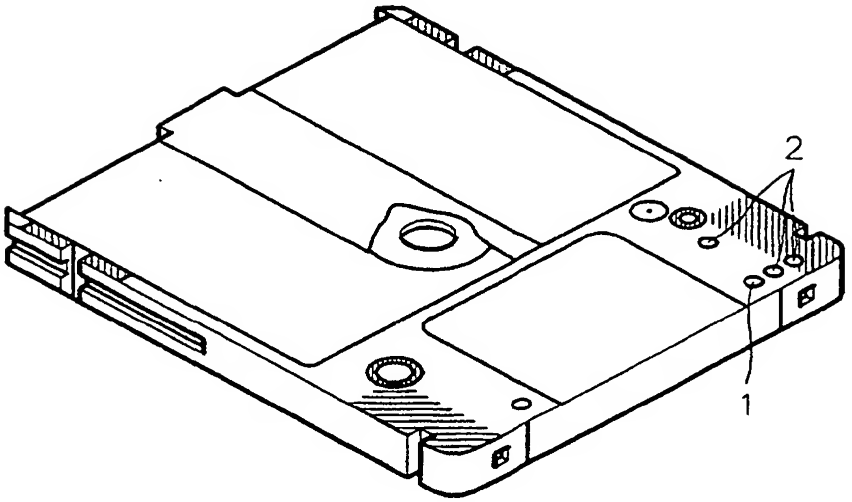


FIG. 2

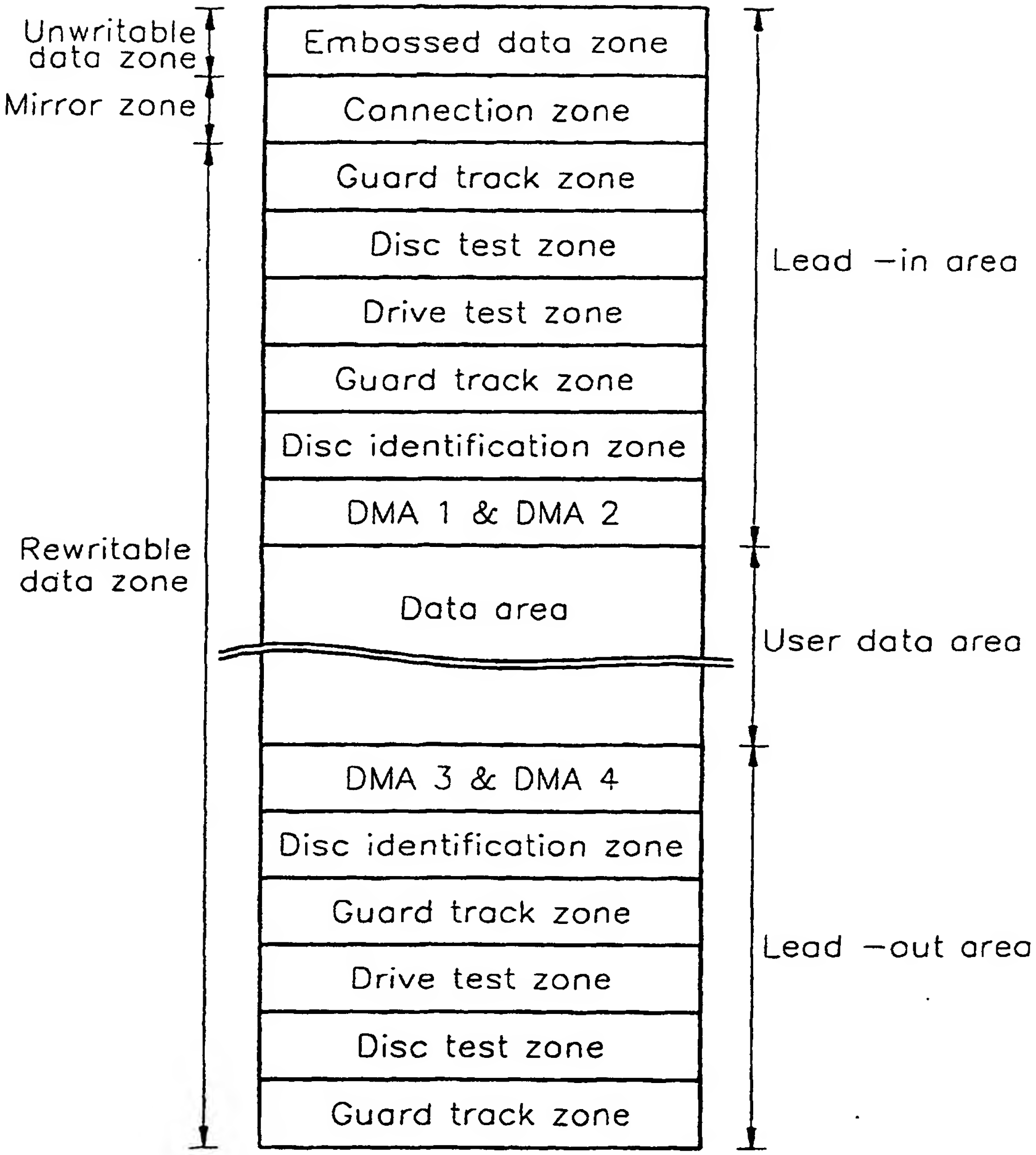

Unwritable data zone
Mirror zone
Rewritable data zone
Embossed data zone
Connection zone
Guard track zone
Disc test zone
Drive test zone
Guard track zone
Disc identification zone
DMA 1 & DMA 2
Data area
DMA 3 & DMA 4
Disc identification zone
Guard track zone
Drive test zone
Disc test zone
Guard track zone
Lead -in area
User data area
Lead -out area

FIG. 3A

b7	b6	b5	b4	b3	b2	b1	b0
In Process			Reserved			User certification	Disc manufacturer certification

FIG. 3B

b7	b6	b5	b4	b3	b2	b1	b0
In Process		Reserved				User certification	Reserved

FIG. 4A

b7	b6	b5	b4	b3	b2	b1	b0
In Process			Disc write protection		Reserved	User certification	Disc manufacturer certification

FIG. 4B

b7	b6	b5	b4	b3	b2	b1	b0
In Process		Reserved	Group write protection		Reserved	User certification	Reserved

FIG. 5A

b7	b6	b5	b4	b3	b2	b1	b0
In Process			Disc write protection	Reserved		User certification	Disc manufacturer Certification

FIG. 5B

b7	b6	b5	b4	b3	b2	b1	b0
In Process		Reserved	Group write protection	Reserved		User certification	Reserved

FIG. 6

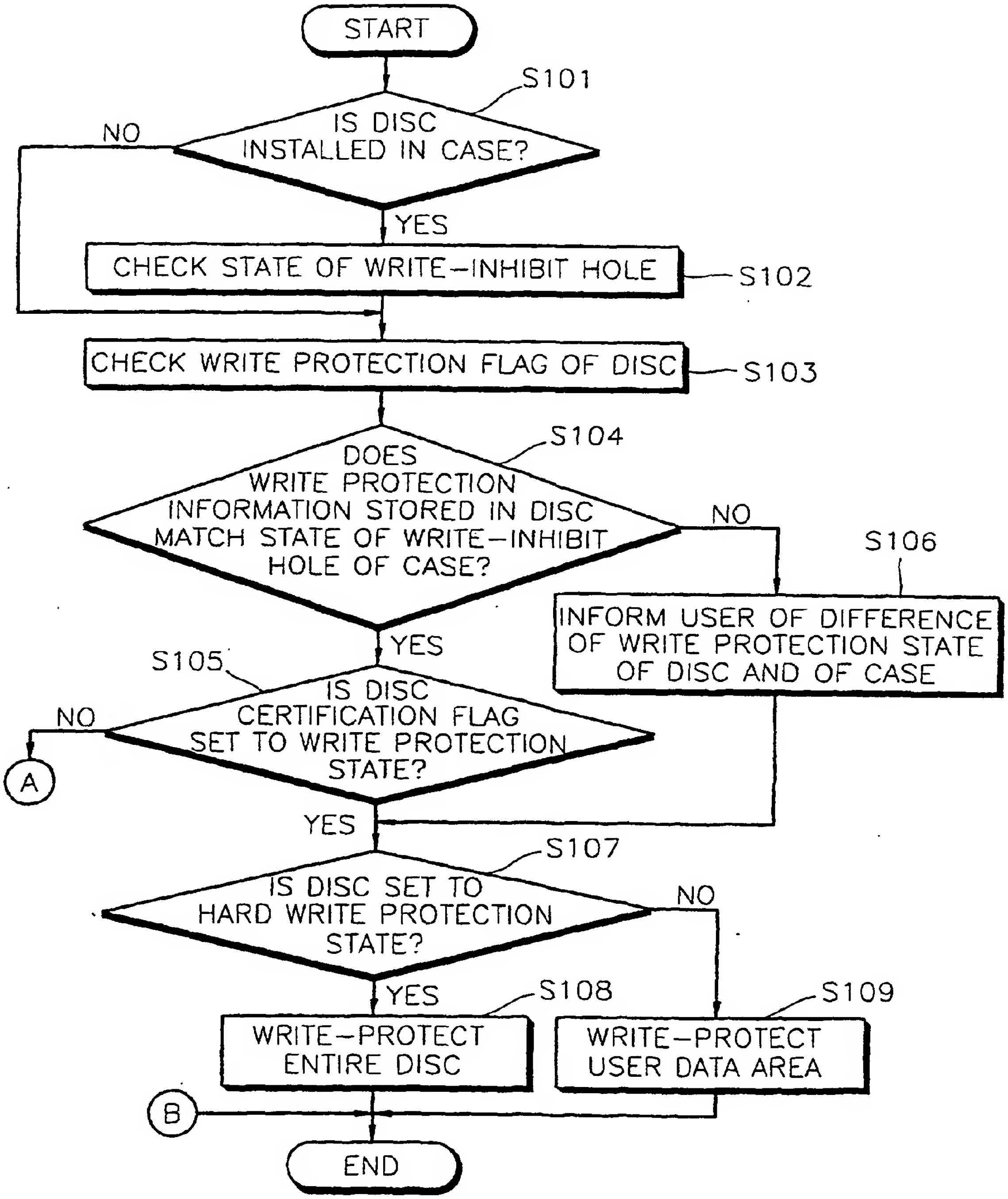

START
S101
IS DISC INSTALLED IN CASE?
NO
YES
CHECK STATE OF WRITE-INHIBIT HOLE
S102
CHECK WRITE PROTECTION FLAG OF DISC
S103
S104
DOES WRITE PROTECTION INFORMATION STORED IN DISC MATCH STATE OF WRITE-INHIBIT HOLE OF CASE?
NO
S106
INFORM USER OF DIFFERENCE OF WRITE PROTECTION STATE OF DISC AND OF CASE
YES
S105
IS DISC CERTIFICATION FLAG SET TO WRITE PROTECTION STATE?
NO
A
YES
S107
IS DISC SET TO HARD WRITE PROTECTION STATE?
NO
YES
S108
WRITE-PROTECT ENTIRE DISC
S109
WRITE-PROTECT USER DATA AREA
B
END

FIG. 6 (CONTINUED)

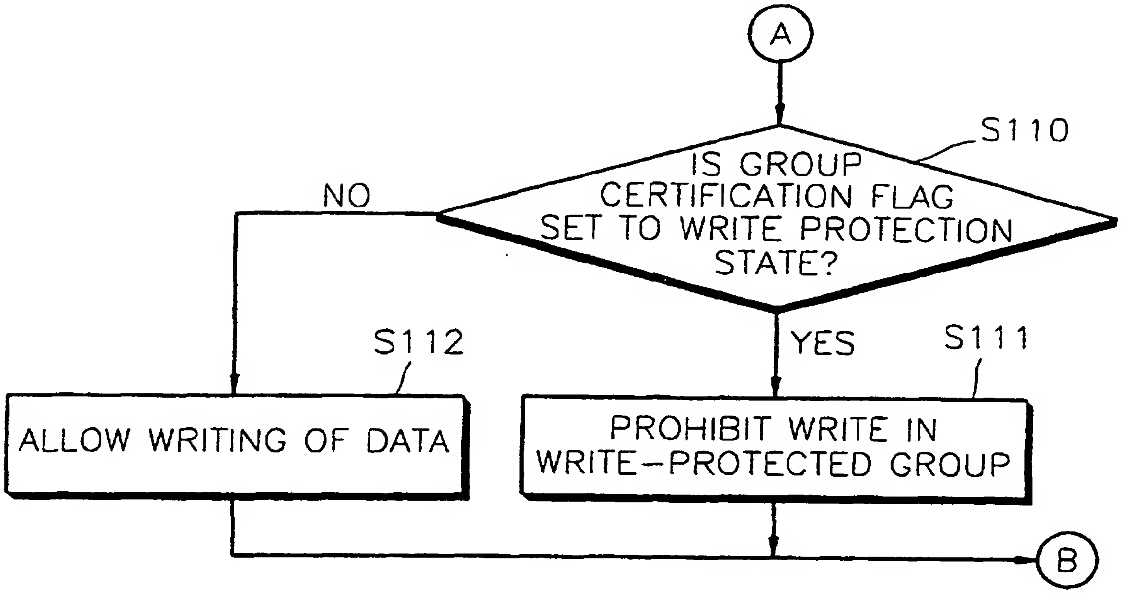

A
S110
IS GROUP CERTIFICATION FLAG SET TO WRITE PROTECTION STATE?
NO
YES
S112
ALLOW WRITING OF DATA
S111
PROHIBIT WRITE IN WRITE-PROTECTED GROUP
B

FIG. 7

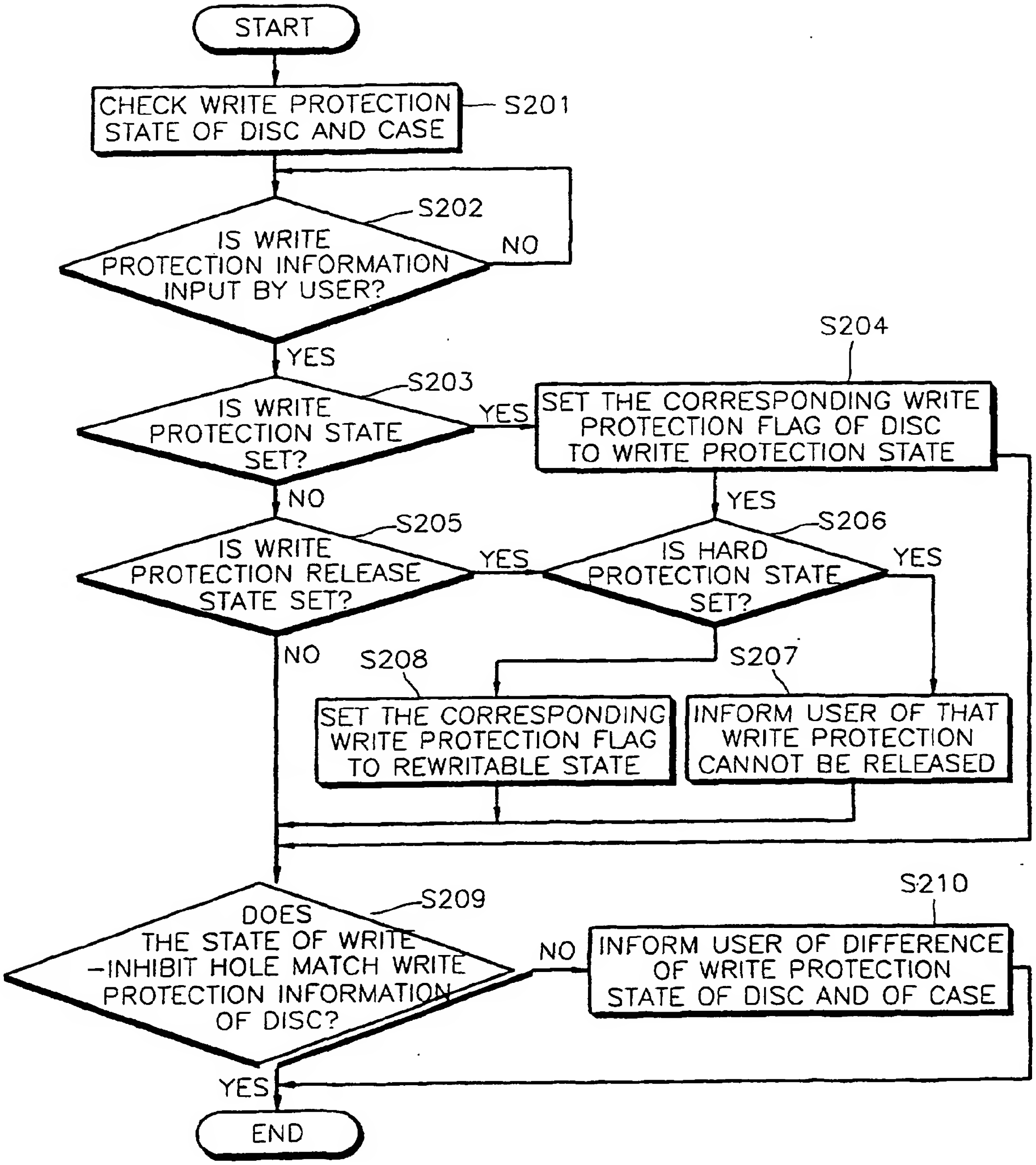

START
CHECK WRITE PROTECTION STATE OF DISC AND CASE
S201
IS WRITE PROTECTION INFORMATION INPUT BY USER?
S202
NO
YES
IS WRITE PROTECTION STATE SET?
S203
YES
SET THE CORRESPONDING WRITE PROTECTION FLAG OF DISC TO WRITE PROTECTION STATE
S204
NO
IS WRITE PROTECTION RELEASE STATE SET?
S205
YES
IS HARD PROTECTION STATE SET?
S206
YES
YES
NO
S208
SET THE CORRESPONDING WRITE PROTECTION FLAG TO REWRITABLE STATE
S207
INFORM USER OF THAT WRITE PROTECTION CANNOT BE RELEASED
DOES THE STATE OF WRITE-INHIBIT HOLE MATCH WRITE PROTECTION INFORMATION OF DISC?
S209
NO
INFORM USER OF DIFFERENCE OF WRITE PROTECTION STATE OF DISC AND OF CASE
S210
YES
END

FIG. 8

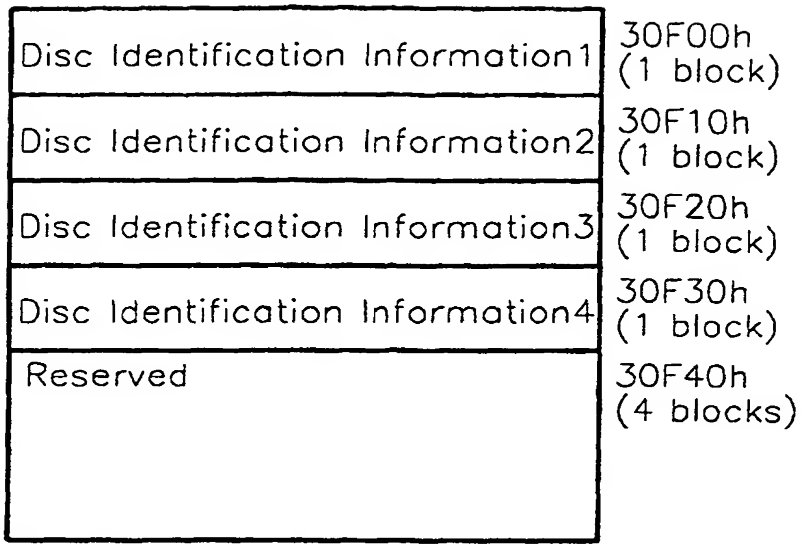

Disc Identification Information1
30F00h
(1 block)
Disc Identification Information2
30F10h
(1 block)
Disc Identification Information3
30F20h
(1 block)
Disc Identification Information4
30F30h
(1 block)
Reserved
30F40h
(4 blocks)

FIG. 9

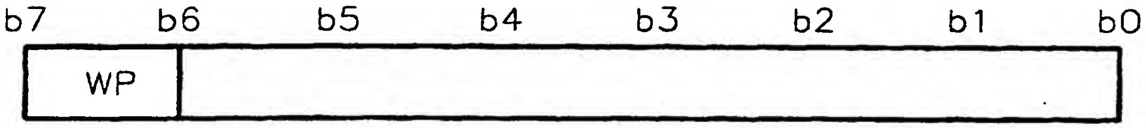

b7
b6
b5
b4
b3
b2
b1
b0
WP

FIG. 10

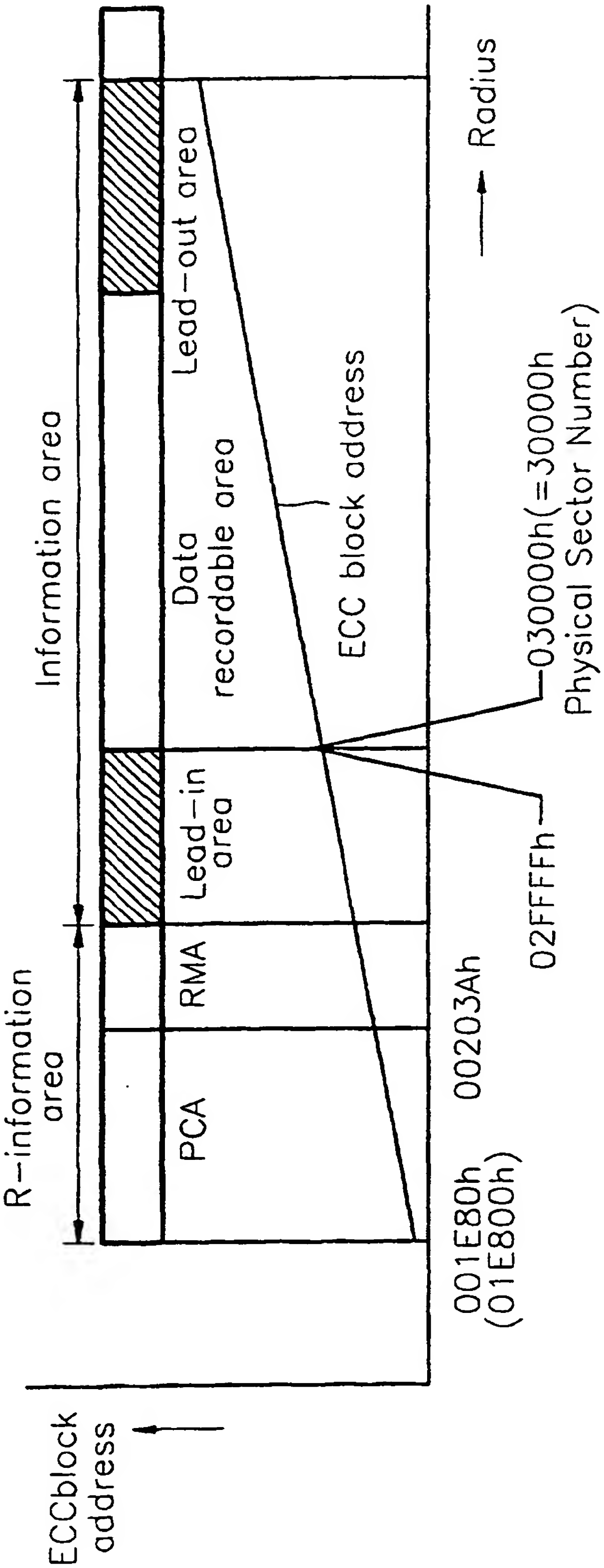

R-information area
Information area
PCA
RMA
Lead-in area
Data recordable area
Lead-out area
ECC block address
001E80h (01E800h)
00203Ah
02FFFFh
030000h(=300000h Physical Sector Number)
Radius
ECCblock address

FIG. 11

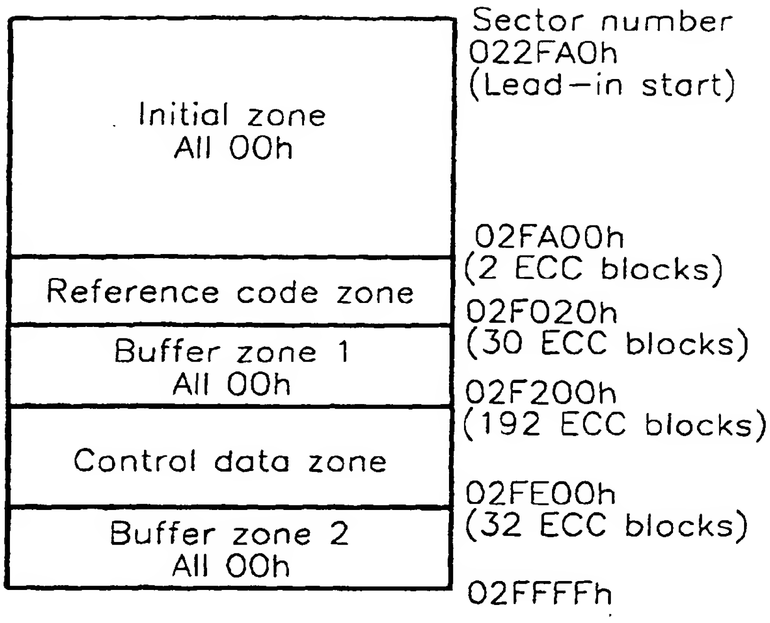

Sector number
022FA0h
(Lead−in start)
Initial zone
All 00h
02FA00h
(2 ECC blocks)
Reference code zone
02F020h
(30 ECC blocks)
Buffer zone 1
All 00h
02F200h
(192 ECC blocks)
Control data zone
02FE00h
(32 ECC blocks)
Buffer zone 2
All 00h
02FFFFh

FIG. 12

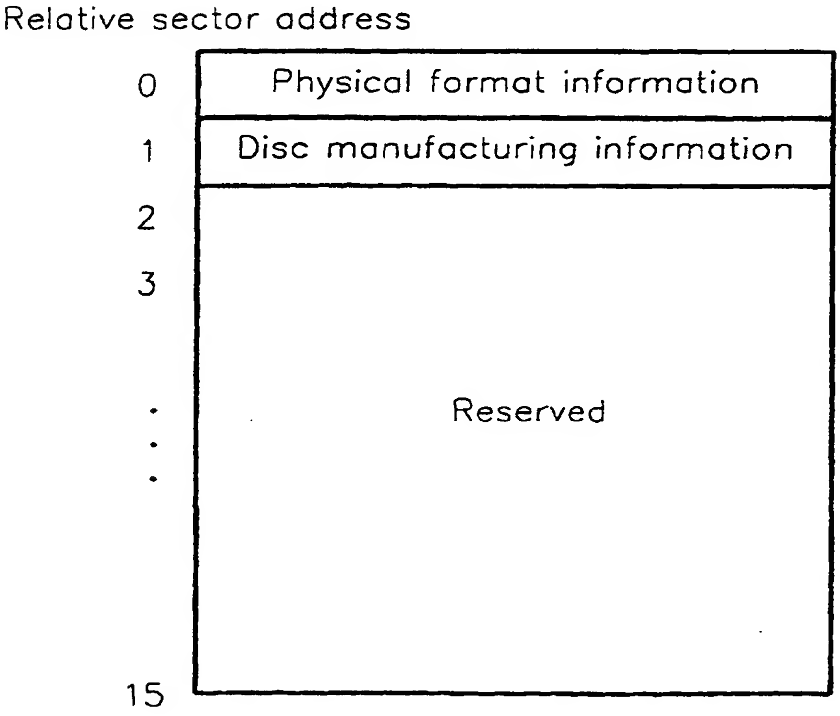
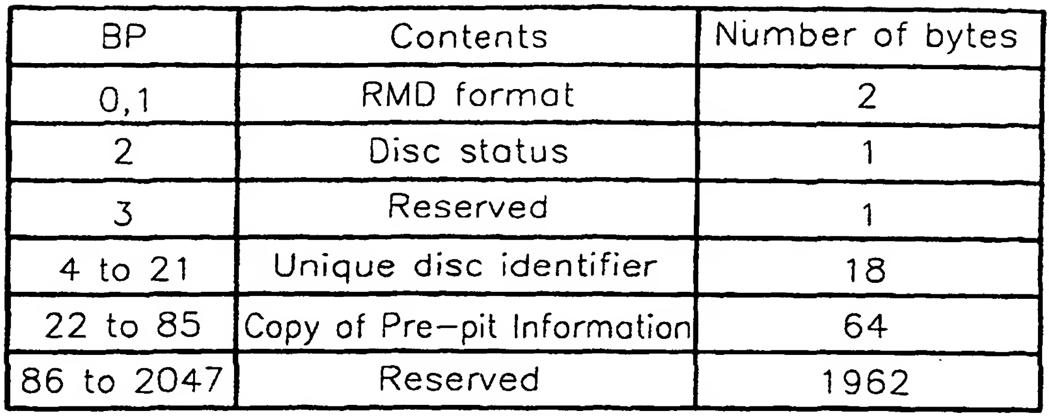

Relative sector address
0
Physical format information
1
Disc manufacturing information
2
3
Reserved
15

FIG. 13

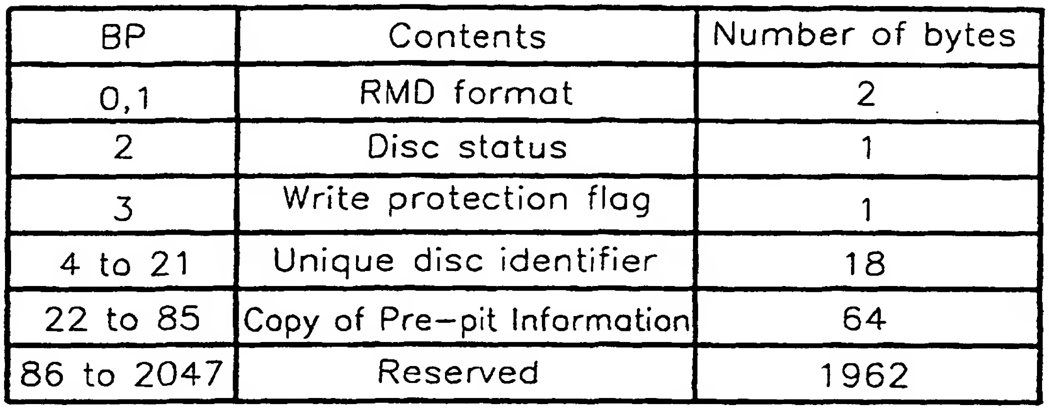
Sector #	RMD Field	DVD-R(Ver 1.9)	DVD-RW
0		Linking-loss area	
1	0	General information of disc	
2	1	OPC related information	
3	2	User specific data	
4	3	Border zone information	
5	4	Rzone information	RZone information
6	5		Defect management & certification related information
7	6		
8	7		
9	8		
10	9		
11	10		
12	11		
13	12		
14	13	Reserved	
15	14		

FIG. 14



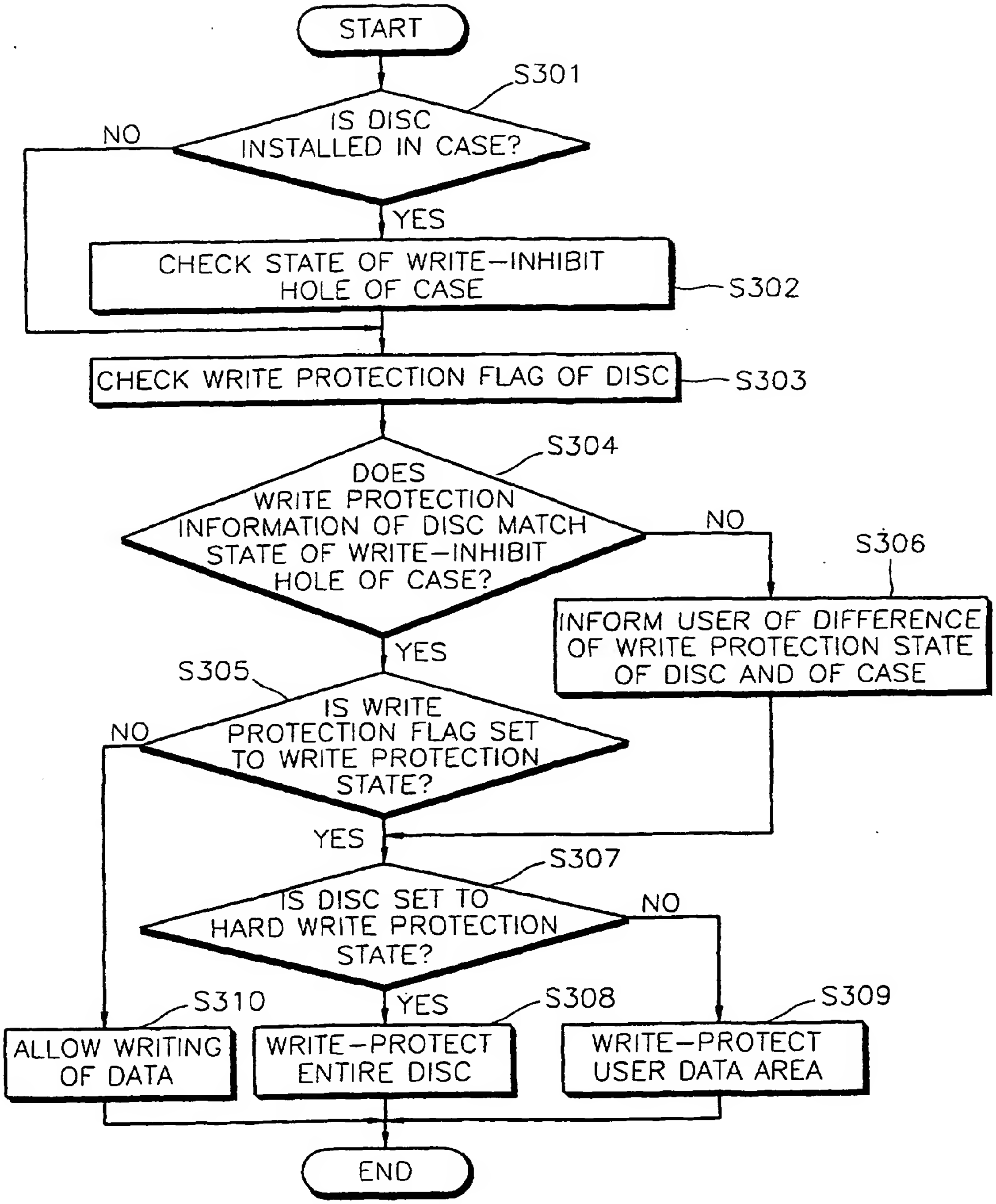
BP	Contents	Number of bytes
0,1	RMD format	2
2	Disc status	1
3	Reserved	1
4 to 21	Unique disc identifier	18
22 to 85	Copy of Pre-pit Information	64
86 to 2047	Reserved	1962

FIG. 15



BP	Contents	Number of bytes
0,1	RMD format	2
2	Disc status	1
3	Write protection flag	1
4 to 21	Unique disc identifier	18
22 to 85	Copy of Pre-pit Information	64
86 to 2047	Reserved	1962

FIG. 16


START
S301
IS DISC INSTALLED IN CASE?
NO
YES
CHECK STATE OF WRITE-INHIBIT HOLE OF CASE
S302
CHECK WRITE PROTECTION FLAG OF DISC
S303
S304
DOES WRITE PROTECTION INFORMATION OF DISC MATCH STATE OF WRITE-INHIBIT HOLE OF CASE?
NO
S306
INFORM USER OF DIFFERENCE OF WRITE PROTECTION STATE OF DISC AND OF CASE
YES
S305
IS WRITE PROTECTION FLAG SET TO WRITE PROTECTION STATE?
NO
YES
S307
IS DISC SET TO HARD WRITE PROTECTION STATE?
NO
S310
YES
S308
S309
ALLOW WRITING OF DATA
WRITE-PROTECT ENTIRE DISC
WRITE-PROTECT USER DATA AREA
END